WHITEPAPER

Things CISOs Need to Know Before Choosing a CAASM Solution

Everything You Need to Know But Don't Have Time to Research About CAASM.

LUCIDUM

A Quick, Functional Definition of CAASM

Many cybersecurity professionals have probably run across CAASM in their daily IT digests orwithin a webinar they've attended recently. But can it work for you?

First, let's define CAASM. No, it's not a poor attempt at spelling chasm establishing ametaphorical digital acronym of a deep cyber fissure in your IT asset ecosystem.

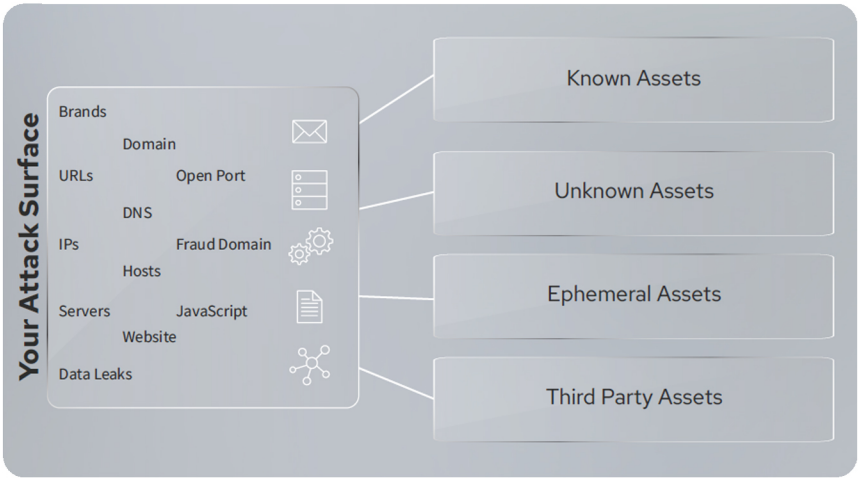
CAASM stands for **Cyber Asset Attack Surface Management.** *The current, most widely accepted definition comes from Gartner, where they articulate it is a "technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges."*

What does it do? Gartner explains: *"It enables organizations to see all assets (both internal and external) through API integrations with existing tools, query against the Consolidated data, identify vulnerabilities and gaps in security controls, and remediate issues."*

But do I need it? Gartner says: *"... drivers for CAASM include the need for full visibility into assets, quicker and more accurate audit compliance reporting, improved security posture, and consolidated asset views for multiple teams across an organization."*

The Value of CAASM to Your Organization

So, thanks, Gartner, for that. But, is this just another attempt at BuzzWord Bingo or does it mean something more? Is it something different – and does it really have any value to me in my organization?



LUCIDUM

Problems Solved by CAASM

In order to understand CAASM, it's helpful to pick apart the problem CAASM solutions are addressing. **Visibility and Management.**

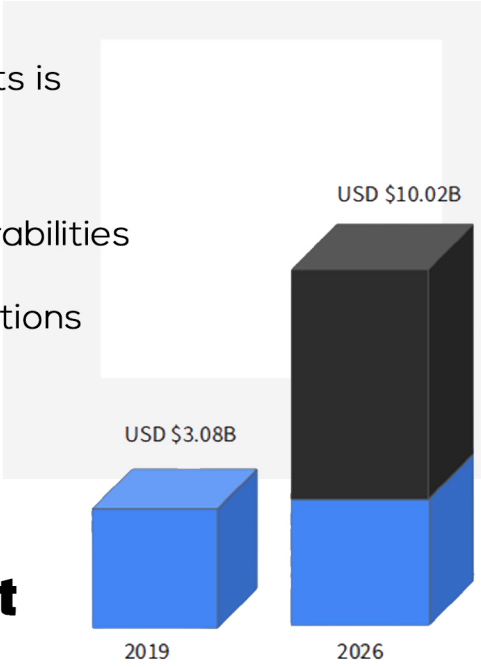
IT assets are ever changing, and more than ever before, being deployed at a rapid rate. The global digital asset management market is expected to grow at a compound annual growth rate of 18.36% to reach a market size of over $10 billion in 2026, up from just over $3 billion in 2019.

The market is expected to surge in the coming years, because of the rise in cloud deployment across various enterprises Worldwide. IoT device growth, edge computing, BYOD, remote workforce, mobile devices, and 5G are all contributors to asset sprawl and growth.

The rapidly growing number of assets is also fueling the problems of:

- Limited asset visibility
- Increased asset risks and vulnerabilities
- Reduced security controls
- Management of asset configurations

This is where CAASM can help.



Digital Asset Management Market

Market forecast to grow at a CAGR of 18.4%

https://www.researchandmarkets.com/reports/5457527

As we look at the problems that CAASM solutions address, the most effective CAASM solutions understand that problem solving is not a "one-size-fits-all" process. They know that actionable intelligence depends on the situation and relationship of the assets, users, and what data those users interact with.

The best CAASM solutions help you make better decisions because they adapt their approach to ever developing environments - and they are powered by Artificial Intelligence (AI) and Machine Learning (ML). Why? Because there is too much information and data to manage with just humans alone using manual or semi-manual processes to track and organize complex ecosystems.

LUCIDUM

How Cynefin and CAASM Work Together

The best CAASM tools are the ones that leverage the problem solving methodology established within "The Cynefin Framework," which was created at IBM by Dave Snowden in 1999.

Fun fact: "Cynefin" is pronounced "ku-nev-in" and is a Welsh word that translates to "place" or "habitat".

It took 8 years, but Snowden and his colleague, Mary Boone, published the framework in 2007 where it was featured in the Harvard Business Review. Within the framework are five decision-making contexts or "domains":

- Clear
- Complicated
- Complex
- Chaotic
- Disorder

These domains can help you identify and articulate how you perceive situations and make sense of your assets and users' behaviors on a continual basis using AI/ML. The framework draws on research into systems theory, complexity theory, network theory, and learning theories, which provide insights and the basis for how humans and machines learn and how they differ from one another. They also address how small parts of complex systems fit into large environments. **CAASM tools are set up to eliminate challenges within these domains when the problems are:**

- **Clear:** Where cause-and-effect relationships exist, are predictable, and are repeatable.
- **Complicated:** Where cause and effect relationships are not self-evident, and therefore requires expertise to decipher.
- **Complex:** Where cause and effect are only obvious in hindsight and present unpredictable, emergent outcomes.
- **Chaotic:** Where you don't know which domain the problem lives.
- **Disordered:** Where indecision, confusion, and frustration thrive.

LUCIDUM

CAASM in Action - How it Works With Server Assets

Let's walk through "a day in the life of a server asset" under each of these domains and describe how CAASM in the real world addresses each use case.

Clear:

Use Case Example: a cloud server/instance/vm gets deployed off a base, golden hardened image, in a pre-approved location, assigned to the correct owners with correct permissions every time new resources are needed.

Some may argue, "how is this a problem? That sounds like music to my ears." Well, at face value it might sound that way, but the challenge for CAASM is ensuring identification, discovery, alignment, and accuracy of the asset with its accompanying owners, policy, life cycles, etc. always happens.

There are patterns and relationships that make these types of assets the ones that are rarely missed. These are the ones that organizations will hang their hats on, saying "we got this one. Box checked."

Although the best practices for discovery, lassification, and response behaviors are in place, without CAASM tools, it is still a manual process that can lead to human error and data integrity problems.

CAASM automates and, more Importantly, validates policies, procedures, and asset lifecycle management.

LUCIDUM

Complicated:

Use Case Example: a cloud server/instance/vm gets deployed, more than one storage asset gets mounted/attached to the server, (such as an EBS volume and RDS Instance, and S3 Bucket) to leverage the value of cloud for cost performance, time to market, and application benefit.

When the server is decommissioned or scaled up or down, assets (or servers) sprawl or are orphaned. These quickly add up and expose you to risks, security issues, non-compliance, and negative financial impact.

CAASM provides discovery, identification, and relationship access views to ensure no asset entity is left behind, exposed, or in a failed compliant state. CAASM keeps a finger on the pulse of each of these relationships and understands when changes happen. It will then provide actionable intelligence on what steps are needed.

CAASM solutions can auto-remediate the issue for and on behalf of the organization. More advanced CAASM solutions will allow you to take preventive actions based on machinelearned behaviors so that no remediation is required.

Complex:

Use Case Example: a cloud server is deployed based on cloud provider instance type (configs, location, and cost/performance, e.g. t2.micro). Later, it is retired, and that instance is transferred, decommissioned, and redeployed to a new instance type with different config, location, and cost/performance profile.

The problem is that suddenly, what you thought you knew has exchanged places and pieces with other things you thought you knew - and now you're getting mixed signals or worse, you don't know what's happening or what has happened.

This type of use case example could be forced upon the organization based on the cloud provider retiring older infrastructure and instance types. The more prevalent driver may be new compliance requirements that force you to decommission and redeploy in various ways.

CAASM addresses this problem by active discovery of new instance types and classification automatically, to future proof your deployments. Further, it understands the relationships between the retired assets to the new assets. The actionable intelligence in complex problems can drive automated change controls and CI and CMDB synchronization.

LUCIDUM

Chaotic:

Use Case Example: a cloud server isn't a cloud server at all but uses an Infrastructure as Code.

Organizations are blind to knowing what it is, where it is, or when it is active because it is not a server. It is, instead, a slippery, ephemeral service such as a microservice. The more ephemeral the asset, the more chaotic and challenging the problem becomes.

How do we address new asset types when we don't know how they act under traditional paradigms? What if their natural state is constantly changing?

CAASM addresses the chaotic by looking at all services and the users of those services and their behaviors so that they can be discovered, classified, and tracked. It is not just looking at a limited set of cloud services – it is automatically taking the chaos out of chaotic challenges.

Disorder:

You may be asking about the Disorder domain in the middle. That is the space where indecision, confusion, and frustration thrive. With the right CAASM solution, the fear of Disorder for CISOs is a thing of the past and doesn't have a place when deployed.

In moving through the domains, with the proper CAASM solution in place you will move in a clockwise direction from Chaotic through Complex and Complicated, and find yourself at Simple. Without a CAASM solution, rules and policy/procedure will allow the process to slip, forcing a counter-clockwise movement and backward drift to Chaotic, and potentially Disorder.

LUCIDUM

Choosing a CAASM Solution Provider

CAASM solutions that provide complete asset discovery and eliminate blind spots across cloud, security, and IT operations are the table stakes. They must know how to tackle the hard problems by understanding the requirement of doing more than just identifying and classifying assets.

The best CAASM solutions provide actionable intelligence, whether they are supplied with problems that are CLEAR, COMPLICATED, COMPLEX, or CHAOTIC.

Here are the must have attributes of a successful CAASM solution for both the short and long term.

No more unknowns: CAASM solutions must authenticate to all of your security,infrastructure, cloud, and management solutions. They must reveal each and every asset, who, and how they are interacting with each other all the way down to which files they accessed and when.

Out of the box actionable intelligence: CAASM solutions should provide common use-case problems solved out of the box. They should let the user refine the views into the respective environments. A user should only be expected to have to tune the last 5-10%.

Automatic machine-learned actions for audits and compliance prevention and mitigation: With a holistic view of all assets, combined with Machine Learning, the solution should be able to understand how assets either adhere to or deviate from policies and procedures. No more full-time employees chasing audits and war room triage.

The more ephemeral the workloads, assets, and users become, the more vital the need for leveraging Machine Learning is to the success of a CAASM solution. Manual rules and manual tuning require experts in each asset class and user type to ensure the rules are correct and that they are constantly continuing to tune as things adapt. The prime value of Machine Learning is that it automatically solves the need for tuning.

LUCIDUM

Open API: Although CAASM solutions can curate, transform, and build dynamic relationships across all your data streams, knowing if data isn't locked in is critical. CAASM solutions should be used daily but the value of the solution really comes in by enriching other operating tools, such as your ticketing systems, CMDBs, finance tools, and other day-to-day operating platforms.

A CAASM solution that tailors, refines, and enriches data, and can then be leveraged by the other systems to keep the enterprise in sync with accurate information, is a must.

In Closing

These examples address the discovery, classification, and identification of the knowns and unknowns in their four possible states: Clear, Complicated, Complex, or Chaotic.

True CAASM solutions must have these table stake capabilities. There are many dimensions, relationships, and opportunities besides physical and virtual assets. As we alluded to, the human element is a key in CAASM solutions. The human/user lens of an asset itself, as well as how the user interacts with other assets, is vital in covering the complete cyber asset attack surface area.

The same logic of Cynefin Framework layers should be applied in the same fashion for CAASM solutions for the human element and relationships to the rest of the ecosystem. The patterns and the anti-patterns of "John Doe" day in the life access to systems, and the relationship he has with those assets, are vital for success with CAASM.

As you select the right CAASM solution; focus on your use cases, and how they align to the level of discovery, classification, automation, and predictive preventive management you have need of, not just today, but look at the chaotic nature of the future. Without CAASM, your only sane option is to run away.

Lucidum can affirm Gartner's position that the CAASM market is rapidly growing. CISOs who don't have a CAASM strategy, or those who have attempted to address CAASM on their own, are actively investing in CAASM solutions like Lucidum to ensure there is **limitless asset visibility.** Contact us if you would like to learn more.

LUCIDUM

About Lucidum

Lucidum is the AI-powered asset discovery company that eliminates blind spots across cloud, security, and IT operations through a patent-pending machine learning and proprietary data ingestion platform. Fortune 500 companies leverage Lucidum's limitless visibility to discover, triangulate, and identify all cyber assets, even those previously unknown, and take action by prioritizing and mitigating risks. For more information about how Lucidum can help secure, manage, and transform your enterprise, visit lucidum.io.

LUCIDUM